

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

BLOCKCRUSHR INC.,

Plaintiff,

v.

CONSENSYS INC., CONSENSYS FUND I, L.P.,
CONSENSYS DILIGENCE, INC., CONSENSYS
GP I, LLC, and CONSENSYS VENTURES LLC,

Defendants.

Case No. 20-cv-3134-FB-RLM

AGREEMENT REGARDING DISCOVERY OF
ELECTRONICALLY STORED INFORMATION AND
PROPOSED ORDER

Pursuant to Federal Rule of Civil Procedure 29, this Agreement Regarding Discovery for Electronically Stored Information (the “Agreement”) is entered into by and among the named Parties in the above-captioned action, through their respective counsel of record. Nothing in this Agreement shall negate any objections or limitations in any response to a request for production of documents.

1. Definitions: For purposes of this Agreement:

(a) “Document” or “documents” is defined to be synonymous in meaning and equal in scope to the usage of this term in Federal Rules of Civil Procedure 26 and 34 and Local Civil Rule 26.3.

(b) “Email” means electronic messages sent or received asynchronously, including any documents incorporated as attachments, including, but not limited to, industry standard applications like Microsoft Outlook, Google Gmail or Lotus Notes, as well as non-standard applications like protonmail or anonymous speech.

(c) “ESI” is an abbreviation of “electronically stored information” and shall have the same meaning and scope as it has in the Federal Rules of Civil Procedure.

(d) “Extracted Text” means the text extracted from a Native Format file and includes at least all header, footer and document body information.

(e) “Hard Copy Document” means a Document that was maintained in paper form at the time this Agreement was entered.

(f) “Load File” means an electronic file that is used to import all required production information into a document database, including document images, extracted or OCR text, native files where required, and metadata, as well as information indicating document and page breaks, and document relationships such as those between an email and its attachments and between a document and information related to embedded content.

(g) “Metadata” means structure information about ESI that is created by the file system or application, embedded in the Document or Email and sometimes modified through ordinary business use. Metadata of the ESI describes, inter alia, the characteristics, origins, usage and validity of the collected ESI.

(h) “Native Format” means the format of ESI in the application in which such ESI was originally created.

(i) “OCR” means the optical character recognition technology used to read electron images of Hard Copy Documents and to output readable content of such documents to a searchable text format. The latter text is also referred to as the “OCR text” or simply “OCR”.

(j) “Party” or “Parties” means, individually or collectively, the Plaintiff and Defendants in the above-caption matter.

(k) “Producing Party” means a Party that produces documents.

(l) “Receiving Party” means a Party to whom documents are produced.

(m) “Tagged Image File Format.” “TIFF,” “.TIFF,” or “.TIF” refers to the CCITT Group IV graphic file format for storing bit-mapped images of ESI or Hard Copy Documents.

2. Scope

(a) The procedures and protocols set forth in this Agreement shall govern the format and processing of common-place Documents or standard ESI (such as emails, Microsoft Office documents, WordPerfect documents, .pdfs, text messages, internet history) produced by the Parties in the above-caption matter, to the extent available. Any practice or procedure set forth herein may be modified only by written agreement of the Parties.

(b) The Parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of Documents, including, without limitation, objections regarding the burden, overbreadth, or relevance of document requests related to Documents. This Agreement does not define the scope of production nor the relevance of any particular information. The discovery requests, objections thereto, agreements of the Parties, and any related Court orders in the above-captioned matter shall govern the scope of documents to be produced.

(c) Nothing in this Agreement is intended to alter the Parties’ obligations under Federal Rule of Civil Procedure 26(b)(2)(B) and 34(a)(1), or any applicable Local Rule.

(d) Nothing in this Agreement is intended to be an exhaustive list of discovery obligations or rights of a Producing Party or a Requesting Party. To the extent additional obligations or rights not addressed in this Agreement arise under the Federal Rules of Civil Procedure, local rules, or applicable state and federal statutes, they shall be controlling.

(e) The Parties shall make reasonable efforts to comply with and resolve any differences concerning compliance with this Agreement. If the Parties are unable to reach agreement, the Parties shall submit any dispute to the Magistrate Judge.

3. **Electronic Discovery - The Collection of ESI**: In a joint effort to balance the volume, relevance, and costs of the production and review process, the Parties stipulate to the following involving the handling and production of electronically stored information (“ESI”).

(a) Thirty (30) days from the entry of this Order, Counsel for Defendants and Plaintiff will mutually disclose all repositories of potentially relevant ESI. This disclosure will include identification of all of the following repositories:

- i. email addresses including but not limited to email addresses registered under an alias or shared with another individual or entity;
- ii. laptops, desktops, hard drives, tablets, phones, or any other computing device;
- iii. multi-user messaging platforms (or “chat” platforms), such as Slack or Microsoft Teams;
- iv. cloud storage accounts;
- v. USB, flash drives, CD/DVDs or any other physical ESI storage medium;
- vi. social media accounts;
- vii. intranet or shared servers;
- viii. text messages and voicemails;
- ix. any physical devices or online repositories used to develop or store intellectual property including but not limited to any computer code repositories; and
- x. any unique or proprietary software on which relevant data is stored.

(b) The Parties will work in good faith to identify, discuss, agree upon, and revise, if necessary, the custodial and non-custodial sources of documents from which ESI is collected and reviewed for possible production in the matter to avoid an unduly burdensome production or retrieving a large quantity of non-responsive ESI.

(c) The Parties agree that search terms and other techniques to identify potentially responsive ESI for review and possible production will be useful to allow document production to

complete in a reasonable amount of time.

(d) To the extent practicable, the Parties shall use informal procedures, agreed upon through a meet-and-confer process, for the production of ESI. In the event of a dispute or disagreement, the Parties will meet and confer in a good faith effort to resolve such dispute or disagreement. Further, insofar as this Agreement relates to the general protocol of identifying and producing ESI, any party may bring a motion to modify or clarify the application of this Agreement to particular ESI or otherwise.

(e) This Agreement is designed, and shall be interpreted, to ensure a balance of the needs of the party requesting ESI to obtain relevant documents and information while avoiding unnecessary burdens for the party responding to a request for production or other production requirement. Nothing in this Agreement is intended to be an exhaustive list of discovery obligations of a producing party or rights of the requesting party. To the extent additional obligations or rights not addressed in this Agreement arise under the Federal Rules of Civil Procedure or applicable State or Federal statutes, they shall be controlling. All Parties reserve their rights under the Federal Rules of Civil Procedure for matters relating to the production of information that are not specifically addressed in this Agreement.

(f) Each party shall make a reasonable and diligent effort to search for and collect responsive ESI. The Parties will apply parameters agreed upon by the Parties or as ordered by the Magistrate Judge. If a party identifies ESI from one of its designated custodians that is likely to contain responsive information, but that it claims is not reasonably accessible, it will provide to the other party a description of the source of the ESI that it claims is not reasonably accessible and the basis of the claim that the source is not reasonably accessible, including detailed description of the party's attempts to make the ESI accessible.

(g) A Producing Party is only required to produce a single copy of any document.

A Producing Party may de-duplicate ESI across its custodians or sources, but if that option is exercised, the Producing Party shall identify each custodian who had a copy of the produced document in the CustodianAll field in the Metadata Load File. De- duplication shall be based on MD5 or SHA-1 hash values, and each Producing Party must disclose the methodology it uses to de-duplicate. However, (i) de-duplication shall be performed only at the document family level so that attachments are not de-duplicated against identical stand-alone versions of such documents and vice versa; (ii) attachments to Emails or other Documents shall not be disassociated from the parent Email or Document, even if they are exact duplicates of another Document in the production; and (iii) Hard Copy Documents may not be eliminated as duplicates of responsive ESI if there is anything written on the Hard Copy Document that makes it different from the electronic copy. A party may only de-duplicate “exact duplicate” Documents and may not de-duplicate “near duplicate” Documents, both of the quoted terms in this sentence being given their ordinary meaning in the e-discovery field. Common system files defined by the NIST library (<http://www.nsl.nist.gov/>) need not be produced.

(h) The Parties will make reasonable efforts to ensure that all encrypted or password-protected Documents reasonably believed to contain responsive material are successfully processed for review and production under the requirements of this Agreement, and that any such decrypted Document believed to be non-privileged and responsive is produced. To the extent encrypted or password-protected Documents are successfully processed according to the requirements of this Agreement, the Parties have no duty to identify the prior encrypted status of such Documents. To the extent such Documents are not successfully processed, the Producing Party agrees to: (a) produce a slipsheet for each encrypted or password protected Document that cannot be successfully processed indicating that the Document cannot be decrypted; and (b) provide the metadata for the Document required by Section 7 to the extent it can be reasonably

extracted from the file in its encrypted form. Nothing in this Agreement shall be deemed to require a Producing Party to process or review for production any encrypted files that do not appear reasonably likely to contain responsive material; however, to the extent the document(s) is reasonably likely to contain responsive material, at the request of the Receiving Party the Producing Party shall provide a detailed description of attempts to decrypt the document(s) and production of it in any event. The Parties shall meet and confer regarding any requests that a Producing Party undertake additional efforts to decrypt files after production.

4. Processing Specifications

(a) All ESI shall be processed with a single time zone and a date and time setting that is consistent across each Parties' productions. The time zone used for a production shall be Greenwich Mean Time.

(b) All TIFF images shall display tracked changes, comments, and other rich data as displayed in the Document, regardless of the display setting for this information as last saved by the custodian, to the extent technically possible.

(c) Email threads are email communications that contain lesser-included email communications that also may exist separately in the Party's electronic document collection. The Parties must produce lesser-included emails even if they contain no unique content from the parent thread.

(d) Absent a Party's specific written notice for good cause, the following categories of ESI are presumed to be inaccessible and not discoverable:

- (i) ESI deleted in the normal course of business;
- (ii) Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including (but not limited to) backup tapes, disks, SAN, and other forms of media, and that are substantially duplicative of data that are more accessible elsewhere;

- (iii) Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;
 - (iv) metadata fields such as last-opened or last-printed dates;
 - (v) Electronic data (*e.g.*, call logs, email, calendars, contact data, notes, *etc.*) sent to or from mobile devices (*e.g.*, iPhone, iPad, Android, and Blackberry devices), if a copy of such electronic data is reasonably accessible for production elsewhere (such as on a server, laptop, desktop computer, or 'cloud' storage);
 - (vi) Voicemail, including Telephone or VOIP voice messages, unless the voicemail is recorded in email (automatic email sent to inbox with voicemail recording);
 - (vii) Text messages and instant messages that are not retained in the ordinary course of business;
 - (viii) Server, system, network, or software application logs;
 - (ix) Data remaining from systems no longer in use that is unintelligible on the systems in use;
 - (x) Structural files not material to individual file contents (*e.g.* .CSS, .XSL, .XML, .DTD, *etc.*);
 - (xi) Operating System files that do not store user-created content (*e.g.* CAT, DLL, DMP, EXE, FON, PNF, OPS, SYS *etc.*);
 - (xii) Application source code, configuration, and other similar files necessary for the function of an application that do not store user-created content during ordinary use (*E.g.* BAK, BIN, CFG, DBF, DAT, JS, JSON, JAR, LUA, MSB, RES, WINNT, YTR *etc.*).
- (e) Absent a Party's specific written notice for good cause, no Party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes, as long as such procedure does not conflict with the required litigation hold for this matter.

5. Inadvertent Production of Privileged Information: If any party inadvertently produces in discovery any information subject to attorney-client privilege, work-product doctrine, or any other privilege, protection or immunity, and the requirements of Rule 502(b) of the Federal

Rules of Evidence have been satisfied, the producing party may (promptly upon learning of such production) notify the receiving party(ies) of such production and seek the return and/or destruction of such information as set forth below. Upon such notification: (1) the receiving party(ies) shall promptly destroy all such information (including, without limitation, all originals and copies of any documents containing or comprising such information, and any information incorporated into its own work product); (2) the information (including, without limitation, all originals and copies of any documents containing or comprising such information) shall continue to be privileged, protected, and/or immune; and (3) no use shall be made of such information (including, without limitation, all originals and copies of any documents containing or comprising such information) by the receiving party(ies), nor shall it be disclosed to anyone by the receiving party(ies). The receiving party(ies) shall promptly provide to the producing party a written certification of the complete destruction of such information (including, without limitation, all originals and copies of any documents containing or comprising such information). Nothing herein, however, shall preclude the receiving party(ies) from subsequently challenging that such materials are privileged, or that any such privilege has been waived (on grounds other than the inadvertent production of such materials).

6. Collection and Production of Hard Copy Documents: The Parties agree to conduct a diligent search for and collect reasonably accessible, non-duplicative responsive hard-copy data in the possession of each party. The Parties agree to produce such hard copy documents in single-page TIFF format along with document level OCR text files and the following fields in a Concordance load file as described in Section 8 below:

- (i) Custodian (Name of Custodian from which the file is being produced);
- (ii) BegBates (Beginning Production Number);
- (iii) EndBates (Ending Production Number);
- (iv) Page count;

- (v) OCR text file; and
- (vi) Date

Each party shall bear the cost of converting the hard-copy paper documents it produces to TIFF format and for providing the load file.

7. **ESI - Processing and Production**: The Parties stipulate to the following regarding the processing and production of documents that were originally maintained as ESI, and acknowledge that the Parties are not obligated to populate manually any of the below fields if such fields cannot be extracted from a document, with the exception of the following: (a) BegBates, (b) EndBates, (c) BegAttach, (d) EndAttach fields, (e) Custodian, (f) Paper (Y/N), (g) NativeFile (Y/N), (h) ProdVolume, (i) ParentBates, and (j) AttachBates.

(a) **NON-E-MAIL ESI**: The native format of all non-e-mail ESI will be maintained by each party. Non-e-mail ESI will be produced in both native format and single-page TIFF format (except for non-redacted Excel documents, which shall be produced in native format with a TIFF placeholder pursuant to Section 7(d) hereof) and corresponding document-level extracted text (or OCR for documents that are redacted) with the following metadata fields, to the extent available, in a Concordance load file as described in Section 8 below:

- (i) Custodian (Name of Custodian from which file is being produced);
- (ii) Author (Author of file from properties);
- (iii) Doc Title (Title of file from properties);
- (iv) Doc Subject (Subject of file from properties);
- (v) Created Date (the date the file was created, in YYYYMMDD or MM/DD/YYYY format);
- (vi) Created Time (the time the file was created in HH:MM:SS format);
- (vii) Last Modified Date (the date the file was created in YYYYMMDD or MM/DD/YYYY format);
- (viii) Last Modified Time (the time the file was created in HH:MM:SS format);
- (ix) File Name (name of the file);
- (x) File Ext (extension for the file);

- (xi) File Path (location of the file)
- (xii) Hash (SHA1 or MD5 hash value, or equivalent);
- (xiii) BegBates (beginning production number);
- (xiv) EndBates (ending production number);
- (xv) BegAtt (BegBates of first document in the family)
- (xvi) EndAtt (EndBates of last document in the family)
- (xvii) ParentID (field contains the BegBates for the parent document and is populated for all attachments within the family group);
- (xviii) AttachID (field contains the BegBates number for each attachment within the family group and is populated for the parent document within a family group);
- (xix) Page count;
- (xx) Confidentiality Label (field contains the confidential designation)
- (xxi) For non-redacted Excel spreadsheets only, a native link (path to the native file as included in the production, e.g. A TIFF placeholder with a link to the native files is required.

(b) **ELECTRONIC MAIL (EMAIL):** All unredacted electronic mail shall be produced in both (1) native format and (2) single-page TIFF format with corresponding document-level extracted text (or OCR for redacted documents) with the following metadata fields, to the extent available, in a Concordance-ready load file as described in Section 8 below (except for attachments that are non-redacted Excel spreadsheets, which shall be produced in native format with a TIFF placeholder pursuant to Section 7(d) hereof):

- (i) Custodian (name of custodian from which file is being produced);
- (ii) From;
- (iii) CC;
- (iv) BCC;
- (v) To;
- (vi) Hash (SHA1 or MD5 hash value, or equivalent);
- (vii) Sent Date (date the e-mail was sent in YYYYMMDD or MM/DD/YYYY format);
- (viii) Sent Time (time the e-mail was sent in HH:MM:SS format);
- (ix) Received Date (date the email was received in YYYYMMDD or MM/DD/YYYY format);

- (x) Received Time (time the email was received in HH:MM:SS format);
- (xi) File Ext (extension for the file);
- (xii) BegBates (beginning production number);
- (xiii) EndBates (ending production number);
- (xiv) BegAtt (BegBates of the first document in the family);
- (xv) EndAtt (EndBates of last document in the family);
- (xvi) ParentID (field contains the BegBates for the parent document and is populated for all attachments within the family group);
- (xvii) AttachID (field contains the BegBates number for each attachment within the family group and is populated for the parent document within a family group);
- (xviii) Page count;
- (xix) Email Subject.
- (xx) Header (field containing the physical location of the servers through which the email travelled and the IP addresses associated with those servers)
- (xxi) Confidentiality Label (field contains the confidential designation)

Electronic mail shall be produced along with attachments in sequential order as part of a family, maintaining the parent-child relationship, when either the message or any attachment is responsive. If any message or attachment is responsive but is withheld based on privilege, only the privileged portion may be withheld. In the event a portion of the document is withheld on the basis of privilege, the unredacted portion of the document shall be produced consistent with this section, except that the producing party shall withhold and maintain the native format of the document.

(c) **REDACTED ESI:** Production of redacted ESI shall be subject to the general production requirements set forth herein. For each document that is redacted, the field “Redacted” shall be populated with the value “Yes” and OCR text files of the redacted version of the document shall be provided.

(d) **EXCEL SPREADSHEETS:** All Excel spreadsheets shall be produced in native format with a TIFF placeholder, except if an Excel spreadsheet must be redacted in which case it

shall be produced in TIFF format (provided, however, that if the party receiving a redacted Excel spreadsheet in TIFF format determines that a native version is necessary, the party producing the Excel spreadsheet shall make available a native version of the Excel spreadsheet with any redactions necessary to protect privilege (i.e. not the original native file)). This paragraph shall apply to all such ESI irrespective of whether it takes the form of standalone files or attachments to e-mails or other files. To the extent that any Excel spreadsheet requires a confidentiality legend, the TIFF placeholder shall contain such confidentiality legend, and the filename of the Excel spreadsheet shall also include such confidentiality legend.

(e) **ZIP FILES:** All compressed or zipped ESI shall be unzipped or decompressed before production. To the extent that there are multiple files within a zip folder, each shall be considered a single document with respect to determining responsiveness (unless attached to an email, in which case the protocol in subsection (b) hereof shall apply).

(f) **VIDEO FILES:** Unless otherwise mutually agreed by the Parties, video files are to be produced in the native video file format in which they were maintained in the ordinary course of business, unless redactions are needed. If redactions are needed, the redacted media file may be produced either in the original Native Format or in a standard media format. The Producing Party shall clearly indicate which segments of a video file have been redacted.

(g) **AUDIO FILES:** Audio files are to be produced in the native audio file format in which they were maintained in the ordinary course of business, unless redactions are needed. If redactions are needed, the redacted audio file may be produced either in the original Native Format or in a standard media format. The Producing Party shall clearly indicate which segments of an audio file have been redacted.

(h) To the extent a response to discovery requires a Party to provide documents from a production set of a prior litigation or investigation or documents received from a non-

party through formal subpoena or any informal manner, such Party may produce the documents from the production set as they were produced in the prior action or from the non-party and shall not be required to provide any metadata fields that were not produced in the prior action or provided by the non-party. Notwithstanding this provision, the Parties retain the right to object to the production of documents from prior litigation or investigations.

(i) Nothing in this Agreement shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work product immunity, or any other applicable privilege. The Parties do not waive any objections as to the production, discoverability, admissibility, or confidentiality of Documents or ESI.

(j) The Parties agree to meet and confer in good faith if there are any other file types that encounter difficulties in the production preparation process.

8. Production of ESI & Hard Copy Documents: The Parties agree to the following regarding production of all documents:

(a) The production of all documents shall be in Concordance-ready format and the following load files will be produced:

- (i) Opticon load file compliant with Concordance to load the images;
- (ii) Document level extracted text or OCR (for documents that have been redacted or documents without extractable text);
- (iii) DAT file containing the fields specified herein, with the field names as otherwise provided herein, in the first row. The .DAT file shall be provided with the following hierarchy of delimiters: field - (ASCII 20), quote - (ASCII 254), return value in data - (ASCII 174).

(b) Each page of a produced document shall have a legible, unique page identifier (“Bates Number”) electronically “burned” onto the image. Additionally, any applicable confidentiality legend shall be “burned” into the document image. No other legend or stamp will be placed on the document image other than a confidentiality legend or redactions (where necessary to protect the attorney-client communication privilege, work product doctrine, or other

protection). If the page identifier or legend inadvertently obliterates, conceals, or interferes with any information from the source document, the receiving party shall request and the producing party shall produce a legible copy.

(c) If a Document Number or set of Document Numbers is skipped in a production, the Producing Party shall notify Receiving Party in a cover letter to the production that the production contains skipped Document Numbers and shall identify the skipped numbers. The Document Number shall be placed on the page image in a manner that does not conceal or interfere with any information contained on the page. Each electronic file produced in only Native Format shall be assigned a unique Bates Number and, as applicable, a suitable confidentiality designation, and the database record for that file shall include a single-page TIFF image branded with this unique Bates Number in the lower right corner of the image as a control number, with the phrase “PRODUCED IN NATIVE FORMAT” (or similar language) branded in the center of the page. To protect the confidentiality of files produced in Native Format, any confidentiality designations must appear on the associated TIFF in no less than 12-pt font.

(d) Each page image file shall be named with the unique Bates Number of the page of the document in the case of single-page TIFFs, followed by the extension “.TIF.”

(e) The Producing Party may produce Document images, native files, Load Files, text and/or OCR files, and Metadata on hard drives, CDs, DVDs, hard drive secure FTP, or other mutually agreeable media (“Production Media”). All Production Media must be encrypted, with the encryption code sent by separate email at the time the Production Media is sent to the Receiving Party. Productions made via FTP or other electronic transfer are not required to be supplemented with hard media containing the same Documents. Each piece of Production Media shall include a unique identifying label corresponding to the identity of the Producing Party, the date of the production of Documents on the Production Media and the Bates Number ranges of the Documents

in that production. To the extent that the Production Media includes any confidential information, the label on such Production Media shall indicate that the Production Media includes information so designated. Production Media shall include text referencing the case name and number. Further, any replacement Production Media shall cross-reference the original Production Media, clearly identify that it is a replacement, and cross-reference the Document Number range that is being replaced. All Production Media that is capable of write protection should be write-protected before production.

(f) The Parties shall honor requests for the production of native versions of files and color images to the extent such requests are not unduly burdensome, subject to any necessary redactions to protect the attorney-client or other privileges.

(g) The Parties shall honor requests to make originals of any produced document available for inspection and copying, subject to any necessary redactions to protect the attorney-client or other privileges.

(h) The Parties reserve the right to seek and to object to the costs arising from any discovery or from any improper conduct or bad faith of the litigants.

9. Limits on Scope of Discovery

(a) Limits on E-Mail Discovery. The Parties agree that, with respect to discovery by and among the Parties, e-mail will not be searched or produced, except as follows:

- (i) Specific Requests. To obtain e-mail, the Parties must propound specific e-mail production requests. Any such request shall identify the e-mail custodian and search terms, in accordance with sections 9(b)(ii)-(iv).
- (ii) Custodian Limit. Each of the Parties shall be limited to request ESI from ten (10) custodians.
- (iii) Search Terms. Focused terms, rather than over-broad terms (e.g., product and company names), shall be employed. A single “search term” may consist of a Boolean string containing multiple words and logic limiters to focus the search, rather than a single word. As part of good-faith negotiation of search terms,

the Producing Party will provide a reasonable number of hit reports for the Receiving Party's proposed search terms for a custodian or set of custodians. The Parties agree, however, that once the proposed search terms have been finalized and the Producing Party has made a production, the search terms may not be revised.

- (iv) Search Term Limit. Each of the Parties may only request 20 search terms to be applied to the ESI of each e-mail custodian. That is, a Receiving Party may use a different set of 20 terms for each separate e-mail custodian.
- (v) Document Limit. The total number of e-mail hits, for all custodians collectively, responsive to each Parties' search terms shall not exceed 10,000. The Parties agree to revise their search terms, as necessary, to comply with this limitation.

(b) Limits on "Chat" Discovery and Social Media. The Parties agree that, with respect to discovery by and among the Parties, (i) multi-user messaging platforms (or "chat" platforms), such as Slack or Microsoft Teams and (ii) social media accounts will not be searched or produced unless specifically requested. With respect to any such specific requests, the Parties agree to meet and confer in order to reach agreement on a reasonable scope for any such requests, including with respect to (i) custodians or users, (ii) date ranges, and (iii) search terms.

(c) Modifying the Limits on the Scope of Discovery. The Parties may modify the Limits on the Scope of Discovery only through a showing of good cause. If the Parties do not agree that good cause exists for such modification, the Party seeking modification must make a motion to the Court to demonstrate that good cause exists.

10. Preservation

- (a) Each Party represents that it has taken reasonable steps to preserve reasonably accessible sources of ESI, including implementation of a litigation hold.
- (b) By preserving documents or ESI for the purpose of this Litigation, the Parties are not conceding that such material is discoverable, nor are they waiving any claim of privilege.

Dated: December 11, 2020.

/s/ Kyle W. Roche

Kyle W. Roche
Richard R. Cipolla
Warren Li
ROCHE CYRULNIK FREEDMAN LLP
99 Park Avenue, 19th Floor
New York, New York 10016
(646) 791 6881

Counsel to Plaintiff

/s/ Tibor L. Nagy

Tibor L. Nagy
DONTZIN NAGY & FLEISSIG LLP
980 Madison Avenue
New York, New York 10075
(212) 717-2900
tibor@dnflp.com

Clement Seth Roberts
**ORRICK, HERRINGTON &
SUTCLIFFE LLP**
405 Howard Street
San Francisco, CA 94105
(415) 773-5700
croberts@orrick.com

Laura B. Najemy
**ORRICK, HERRINGTON &
SUTCLIFFE LLP**
222 Berkeley Street, Suite 2000
Boston, MA 02116
(617) 880-1800
lnajemy@orrick.com

Counsel to Defendants

ORDER

Based on the foregoing, it is

SO ORDERED, this _____ day of _____, 2018.

Roanne L. Mann, United States Magistrate Judge